Introduction to the Special Section on Computer Arithmetic

Javier Hormingo (guest editor), Jean-Michel Muller (Supervising TC associate editor), Stuart Oberman (guest editor), Nathalie Revol (guest editor), Arnaud Tisserand (guest editor), Julio Villalba-Moreno (guest editor)

Computer arithmetic is used in many applications, usually totally silently (one should keep in mind that even when running programs that are not at all numeric, memory addresses are computed, which involves additions, multiplications, and sometimes divisions). However, in some areas, it plays a central role. To give a few examples:

- intensive numerical simulations use floating-point arithmetic operations, and elementary functions such as logarithm or cosine. Gaining speed and accuracy is tantamount in these applications;
- cryptographic applications use totally different calculations–but it is still a matter of arithmetic!–, to allow one to efficiently play with elliptic curves, integer lattices, and similar discrete structures.

The major goal is not always speed. Some critical applications require very accurate results, certified bounds, fault-tolerance, or sometimes formally proven algorithms. Embedded computing often requires very low power consumption. As a consequence, computer arithmeticians must design a wide variety of algorithms and (hardware or software) implementations, to address these different issues.

This special issue of IEEE Transactions on Computers follows the 22nd and 23rd editions of the ARITH conferences, held in July 2015 in Lyon, France and in July 2016 in Santa Clara, California, USA. ARITH (the IEEE Symposium on Computer Arithmetic) is the premier international conference in computer arithmetic.

However, this special issue is not a collection of papers presented during these conferences, as they have already been published in the proceedings. The articles presented here are the result of a rigorous selection from more than 30 submitted manuscripts in response to an open call for papers. Authors from 19 countries submitted papers. It is the first time in years that a special section was so successful to require a full special monthly issue to host all the papers.

This special section is the result of a really international and collective effort, and has been made possible thanks to the submitted contributions and to the work of 63 reviewers who wrote 85 reviews: the vast majority of submissions received 3 reviews, only 4 of them received either 2 or 4 reviews. The reviewers did great work and always made pertinent suggestions for improvement: all papers that were not immediately rejected underwent a significant revision. The result was the acceptance of 11 papers. Only 10 of these papers are to be found in this special issue: it was decided that the paper by F. Johansson, entitled *Arb: Efficient Arbitrary-Precision Midpoint-Radius Interval Arithmetic* deserved to be highlighted. As a consequence, it has both been presented as an invited talk at Arith 24 (July 2017, London, UK), and simultaneously published in the August 2017 edition of this journal (Vol. 66, Issue 8, pp. 1281–1292).

In this issue, the reader will discover the following papers.

Floating-point decimal arithmetic is important (indeed, it is frequently mandatory) in financial applications. Besides addition, multiplication is the key operation in these applications. The paper entitled "High Performance Parallel Decimal Multipliers using Hybrid BCD Codes", by Xiaoping Cui, Wenwen Dong, Weiqiang Liu, Earl Swartzlander, and Fabrizio Lombardi, shows a collection of techniques which combined in a novel way produce efficient decimal multipliers.

In lattice-based cryptography, encrypted texts are represented as points near the points of a Euclidean lattice in very-high dimension. They are decrypted using a "round-off" algorithm. The paper "Arithmetical Improvement of the Round-Off for Cryptosystems in High-

- *J. Hormingo and J. Villalba are with University of Malaga, Spain. E-mail: fjhormigo@uma.es, jvillalba@uma.es*
- *J.-M. Muller is with CNRS, Laboratoire LIP, Université de Lyon, Lyon, France. E-mail: jean-michel.muller@ens-lyon.fr*
- *S. Oberman is with NVIDIA, USA. E-mail: stuart.oberman@gmail.com*
- *N. Revol is with INRIA, Laboratoire LIP, Université de Lyon, Lyon, France. E-mail: nathalie.revol@ens-lyon.fr*
- *A. Tisserand is with CNRS, Laboratoire Lab-STICC, Lorient, France. E-mail: Arnaud.Tisserand@univ-ubs.fr*

Dimensional Lattices" by Julien Eynard, Jean-Claude Bajard and Leonel Sousa present interesting refinements that make it possible to reduce the decryption complexity. The authors obtain excellent performance on recent processors.

Implementing fast arithmetic libraries on parallel architectures is a key element for cryptanalysis tools such as the elliptic curve method (ECM). The paper "Fast Modular Arithmetic on the Kalray MPPA-256 Processor for an Energy-Efficient Implementation of ECM" by Jérémie Detrey, Masahiro Ishii, Pierrick Gaudry, Atsuo Inomata, and Kazutoshi Fujikawa presents a highly optimized software support for modular arithmetic on a many-core processor with 256 cores and moduli up to 512 bits, with better performance-energy trade-offs compared to the best state-of-the-art solutions.

Designing arithmetic circuits to be implemented on FPGA is a challenge because the architecture should be adapted to the variety of resources available on the circuit. The paper "Single Precision Logarithm and Exponential Architectures for Hard Floating-Point Enabled FPGAs", by Bogdan Pasca and Martin Langhammer presents new architectures dedicated to the efficient implementation of these functions in novel advanced FPGAs that contain hard floating-point units.

Providing correctly rounded elementary functions in floating-point arithmetic at reasonable cost is difficult. Most currently-used algorithms first evaluate an approximation to the function with a given precision, and if this does not suffice to correctly round the result, perform a significantly more complex calculation. Tuning such algorithms requires having a good estimate of the distribution of the lengths of runs of zeros/ones after the rounding bit of the value of the function at a given floating-point number. For that purpose, a heuristic has been used by many implementers. In the paper "Exponential sums and correctly-rounded functions", Nicolas Brisebarre, Guillaume Hanrot and Olivier Robert use number theory tools to transform that heuristic into a rigorous statement.

The algorithms for evaluating elementary functions often use precomputed tables. In their article "Exact Lookup Tables for the Evaluation of Trigonometric and Hyperbolic Functions", Hugues de Lassus Saint-Geniès, David Defour, and Guillaume Revy propose a general method to use error-free tabulated values. In the particular case of trigonometric and hyperbolic functions, they use Pythagorean triples to design such tables. They illustrate their method in the interesting case of correctly-rounded double-precision functions.

Multiplication by constant numbers or constant matrices is a key operation is signal and image processing. The paper entitled "Optimization of Constant Matrix Multiplication with Low Power and High Throughput" by Martin Kumm, Martin Hardieck, and Peter Zipf presents a new graph-based solution for reducing the cost of circuits implementing multiplications by constant matrices. The reported results show interesting improvements in terms of silicon area, throughput and energy consumption.

In the paper "Efficient Multibyte Floating Point Data Formats using Vectorization", Andrew Anderson, Servesh Muralidharan and David Gregg detail how floating-point data of any precision which is a multiple of 8 between 16 and 64 can be efficiently represented and handled. The use of such formats imply reduced storage and data movement. The corresponding data are efficiently processed by the proposed code generator, and the performances are good, as the accelerators present on many architectures, including Intel's Knight Landing, are well employed.

Division is difficult to implement, and alternatives are often used to avoid it. When the divisor is a small constant, optimized circuits are possible. In the paper "Hardware division by small integer constant", H. Fatih Ugurdag, Florent de Dinechin, Y. Serhan Gener, Sezer Gören, and Laurent-Stéphane Didier consider the Euclidean division of an unsigned integer by a constant. They give new solutions, that involve small look-up tables. They analyze the performancec of three families of techniques.

In the paper "Correctly Rounded Arbitrary-Precision Floating-Point Summation", Vincent Lefèvre presents a fast algorithm together with its low level implementation, for correctly rounded arbitrary-precision floating-point summation in radix 2 arithmetic. His algorithm was implemented in the GNU MPFR library. Each variable (the inputs and the output) can have its own precision.

The guest editors would like to thank the authors for their contribution and diligence at every stage of the review process, and the reviewers for the quality of their reviews and for their feedback that helped much to raise the quality of the final versions of the papers. Last but not least, they are grateful to Paolo Montuschi, Editor-In-Chief of IEEE Transactions in Computers, for offering the opportunity to publish this special issue and for his help and advice during the whole process.

Javier Hormigo received the M.Sc degree and the Ph.D. degree, both in Telecommunication Engineering, from the Universidad de Malaga, Spain, in 1996 and 2000, respectively. He was a member of the Image and Vision Department of the Instituto de Optica, Madrid, Spain, in 1996. He joined the Universidad de Malaga in 1997 and is currently Associate Professor in the Computer Architecture Department. His research interests include computer arithmetic, especially for specific application architectures, and FPGA. Dr. Hormigo served on the program committees for the 22nd and 24th IEEE Symposium on Computer Arithmetic and was program co-chair of the 23rd IEEE Symposium on Computer Arithmetic.

Jean-Michel Muller received the Ph.D. degree in 1985 from the Institut National Polytechnique de Grenoble. He is Directeur de Recherches at CNRS, France. His research interests are in Computer Arithmetic. Dr. Muller was co-program chair of the 13th IEEE Symposium on Computer Arithmetic (Asilomar, USA, June 1997), general chair of the 14th IEEE Symposium on Computer Arithmetic (Adelaide, Australia, April 1999), general chair of the 22nd IEEE Symposium on Computer Arithmetic (Lyon, France, June 2015). He is the author of several books, including "Elementary Functions, Algorithms and Implementation" (3rd edition, Birkhauser, 2016), and he coordinated the writing of the "Handbook of Floating-Point Arithmetic" (Birkhäuser, 2010). He is an associate editor of the IEEE Transactions on Computers, and a fellow member of the IEEE.

Stuart Oberman received the BS degree in electrical engineering from the University of Iowa, Iowa City, in 1992 and the MS and PhD degrees in electrical engineering from Stanford University, Palo Alto, California, in 1994 and 1997, respectively. He is currently Vice President of GPU ASIC Engineering at NVIDIA. He has contributed to the design and verification of seven GPU architectures, and he currently directs multiple GPU design and verification teams. He was program co-chair of the 23rd IEEE Symposium on Computer Arithmetic. He has coauthored one book and more than 20 technical papers. He holds more than 55 granted US patents. He is a senior member of the IEEE.

Nathalie Revol is a research scientist at Inria within LIP laboratory, France. She received the Ph.D. degree from the Institut National Polytechnique de Grenoble in 1994. She has been associate professor at Lille University from 1996 to 2002. She was program co-chair of the 23rd IEEE Symposium on Computer Arithmetic and she served in the program committee for several other editions of the IEEE Symposia on Computer Arithmetic. Since 2008, she chairs the IEEE 1788 working group: this work led to the IEEE 1788-2015 Standard for Interval Arithmetic, and the working group is currently focusing on P1788.1: a simplified standard for interval arithmetic. Indeed, her research interests encompass interval arithmetic, algorithms and applications and related topics such as the use of floating-point arithmetic for implementation issues, variants such as affine arithmetic or Taylor models, and the quality of numerical computations.

Arnaud Tisserand Received the PhD degree From École Normale Supérieure de Lyon, France, in 1997. He is senior researcher at CNRS (French National Center for Scientific Research) in computer science in Lab-STICC laboratory. His research interests include computer arithmetic, computer architecture, digital security, VLSI and FPGA design, design automation, low-power design and applications in applied cryptography, scientific computing, digital signal processing. Dr. Tisserand was program co-chair of the 22nd IEEE Symposium on Computer Arithmetic (Lyon, France, June 2015). He is an associate editor of the IEEE Transactions on Computers, and a senior member of the IEEE.

Julio Villalba-Moreno received the B.S. degree in Physics in 1986 from the University of Granada, and the PhD. degree in Computer Science from the University of Mlaga, Spain. From 1986 to 1991 he worked as a design engineer in the Research and Development Department of Fujitsu, Spain. He joined the Department of Computer Architecture of the University of Malaga in 1986 and is now a Full professor. He has been a member of the Program Committee of the IEEE International Symposium on Computer Arithmetic (ARITH) since 2006. He was an associate Editor of the IEEE Transactions on Computers from July 2011 to June 2015 and served as a Program co-Chair for ARITH22 (Lyon, France, June 22-24, 2015). He is a member of the ARITH steering committee since 2015. He is an associate Editor of the IEEE Transactions on Emerging Technologies in Computing (TETC). His research interests are computer arithmetic formats, application specific architectures and processors and low level FPGA designs.